AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

Claim 1 (Currently Amended) A method of at least partially authenticating a user on a communications network, the method comprising acts of:

(A) ~~transmitting~~ receiving, with a second network device, a first communication from a first network device ~~to a second network device~~, wherein the first communication includes a challenge;

(B) in response to receiving the challenge, generating, with the second network device, a preliminary hash value by performing only a first part of a hash function on a first part of the challenge when the second network device received the challenge via a secure network tunnel between the first network device and the second network device, wherein the first part of the challenge is less than the complete challenge;

(C) transmitting a second communication from the second network device to the first network device via the secure network tunnel, the second communication including the preliminary hash value; ~~and~~

(D) ~~completing performance~~ applying, with the first network device, a remaining part of the hash function to the preliminary hash value, thereby generating a final hash value ~~on the first network device to produce a final hash value.~~; and

(F) authenticating the user based on the final hash value.

Claim 2 (Original) The method of claim 1, wherein act (B) comprises:

performing only part of a Message Digest 5-based encryption function.

Claim 3 (Currently Amended) The method of claim 2, ~~wherein a standard Message Digest 5 algorithm includes adding an appendage of information to information to be communicated to produce padded information that has a length that is a multiple of sixty-four octets, and includes inputting the padded information to a standard Message Digest 5 function, and~~ wherein act (B) comprises:

(1) generating an input sequence to the Message Digest 5-based encryption function by concatenating information to be communicated from the second network device to the first network device; and

(2) inputting the input sequence into the Message Digest 5-based encryption function without previously adding an appendage of information to the input sequence.

Claim 4 (Currently Amended) The method of claim 1, wherein ~~the~~ a complete performance of the hash function ~~involves~~ comprises performing a first number of iterations, wherein act (B) ~~includes~~ comprises performing a second number of iterations that is less than the first number of iterations, and wherein act (D) ~~includes~~ comprises performing a third number of iterations equal to the first number minus the second number, resulting in [[a]] the complete performance of the hash function.

Claim 5 (Currently Amended) The method of claim 1, wherein act (D) includes ~~completing~~ applying the remaining part of the hash function using a second part of the challenge, wherein the first part and the second part form the complete challenge.

Claim 6 (Original) The method of claim 1, wherein act (B) includes generating the preliminary hash value based, at least in part, on the first part of the challenge and a user credential.

Claim 7 (Currently Amended) The method of claim 6, wherein act (B) includes dividing the challenge into the first part and a second part, and the method further comprises:

[[(E)]] configuring the second communication to include an indication of a length in bits of the user credential, and

wherein act (D) includes ~~completing~~ applying the remaining part of the hash function based, at least in part, on the second part of the challenge and the length of the user credential.

Claim 8 (Currently Amended) The method of claim 7, wherein act (D) includes:

(1) determining a state of the hash function based, at least in part, on the length of the user credential; and

(2) ~~completing~~ applying the remaining part of the hash function based, at least in part, on the determined state.

Claim 9 (Currently Amended) The method of claim 7, wherein act (D) further comprises:

(1) determining a length of the second part based, at least in part, on a length of the challenge and the length of the user credential; and

(2) ~~completing~~ applying the remaining part of the hash function based, at least in part, on the determined length of the second part.

Claim 10 (Currently Amended) The method of claim 1, further comprising an act of:

[[(E)]] generating the challenge on the first network device, including generating a portion of the challenge having a length equal to a desired amount of entropy for the challenge, and appending bits to the portion of the challenge to produce the challenge.

Claim 11 (Currently Amended) The method of claim 10, wherein generating the challenge ~~act (E)~~ includes appending sixty-three bits to the portion.

Claim 12 (Currently Amended) The method of claim 1, ~~wherein the challenge includes a plurality of sequences of bits,~~ the method further comprising an act of:

[[(E)]] generating the challenge on the first network device[[,]] such that the challenge ~~including configuring one or more of the~~ includes a plurality of sequences of bits, wherein each sequence of bits in the plurality of sequences of bits ~~to~~ includes at least one non-zero bit.

Claim 13 (Currently Amended) The method of claim 12, wherein each sequence of bits in the plurality of sequences of bits is an octet of bits.

Claim 14 (Currently Amended) The method of claim 1, further comprising an act of:

[[(E)]] generating the challenge on the first network device, including configuring the challenge to include at least a minimum number of octets of bits.

Claim 15 (Original) The method of claim 1, wherein act (B) comprises:

(1) determining a length of a concatenation of an authentication protocol identifier, a user credential and the challenge; and

(2) dividing the challenge into the first part and a second part based on the determined length.

Claim 16 (Canceled).

Claim 17 (Currently Amended) The method of claim 1, wherein the method further comprises an act of:

[[(E)]] transmitting a third communication including the final hash value to a third network device configured to authenticate the user.

Claim 18 (Currently Amended) The method of claim 1, ~~wherein act (A) includes transmitting the first communication within a tunnel between the first network device and the second network device and Act (C) includes transmitting the second communication within the tunnel~~ further comprising generating, with the second network device, a complete hash value by performing all of the hash function on the complete challenge when the second network device receives the complete challenge external to the secure network tunnel.

Claim 19 (Currently Amended) A system for at least partially authenticating a user on a communications network, the system comprising:

a first ~~communication~~ network device ~~operative to~~ that transmits a first communication ~~from a first network device~~ to a second network device, wherein the first communication includes a challenge; ~~and~~

a second network device, ~~operative to~~ that is configured to receive the challenge, to generate a preliminary hash value by performing only a first part of a hash function on a first part of the challenge when the second network device received the challenge via a secure network tunnel between the first network device and the second network device, wherein the first part of the challenge is less than the complete challenge, and to transmit a second communication from the second network device to the first network device via the secure tunnel, the second communication including the preliminary hash value,

wherein the first network device is ~~operative~~ configured to apply a remaining part of the hash function to the preliminary hash value, thereby generating ~~complete performance of the hash function to produce~~ a final hash value; and

an authentication device that authenticates the user based on the final hash value.

Claim 20 (Currently Amended) The system of claim 19, wherein the second network device is operative to perform only part of a Message Digest 5-based encryption function.

Claim 21 (Currently Amended) The system of claim 20, ~~wherein a standard Message Digest 5 algorithm includes adding an appendage of information to information to be communicated to produce padded information that has a length that is a multiple of sixty-four octets, and includes inputting the padded information to a standard Message Digest 5 function, and~~

wherein the second network device is operative to generate an input sequence to the Message Digest 5-based encryption function by concatenating information to be communicated from the second network device to the first network device, and is operative to input the input sequence into the Message Digest 5-based encryption function without previously adding an appendage of information to the input sequence.

Claim 22 (Currently Amended) The system of claim 19, wherein ~~the~~ a complete performance of the hash function ~~involves~~ comprises performing a first number of iterations, and the second network device is operative to perform a second number of iterations that is less than the first number of iterations, and wherein the first network device is operative to perform a third number of iterations equal to the first number minus the second number, resulting in a complete performance of the hash function.

Claim 23 (Currently Amended) The system of claim 19, wherein the first network device is operative to ~~complete~~ apply the remaining part of the hash function using a second part of the challenge, wherein the first part of the challenge and the second part of the challenge form the ~~complete~~ challenge.

Claim 24 (Original) The system of claim 19, wherein the first network device is operative to generate the preliminary hash value based, at least in part, on the first part of the challenge and a user credential.

Claim 25 (Currently Amended) The system of claim 24, wherein the second network device is operative to divide the challenge into the first part and a second part, and to configure the second communication to include an indication of a length in bits of the user credential, and the first network device is operative to ~~complete~~ apply the remaining part of the hash function based, at least in part, on the second part of the challenge and the length of the user credential.

Claim 26 (Original) The system of claim 25, wherein the first network device is operative to determine a state of the hash function based, at least in part, on the length of the user credential, and to complete the hash function based, at least in part, on the determined length.

Claim 27 (Currently Amended) The system of claim 25, wherein the first network device is operative to determine a length of the second part based, at least in part, on a length of the challenge and the length of the user credential, and to ~~complete~~ apply the remaining part of the hash function based, at least in part, on the determined length of the second part.

Claim 28 (Currently Amended) The system of claim 19, wherein the first network device is operative to generate ~~the challenge on the first network device, including generating~~ a portion of the challenge having a length equal to a desired amount of entropy for the challenge, and to append bits to the portion of the challenge, thereby producing ~~to produce~~ the challenge.

Claim 29 (Currently Amended) The ~~method~~ system of claim 28, wherein the first network device is operative to append sixty-three bits to the portion.

Claim 30 (Currently Amended) The system of claim 19, wherein ~~the challenge includes a plurality of sequences of bits, and~~ the first network device is operative to generate the challenge ~~on the first network device, including configuring one or more of~~ such that the challenge includes a ~~the~~ plurality of sequences of bits, wherein each sequence of bits in the plurality of sequences of bits ~~to~~ includes at least one non-zero bit.

Claim 31 (Currently Amended) The system of claim 30, wherein each sequence of bits in the plurality of sequences of bits is an octet of bits.

Claim 32 (Currently Amended) The system of claim 19, wherein the first network device is operative to generate the challenge ~~on the first network device, including configuring~~ such that the challenge [[to]] includes at least a minimum length of bits.

Claim 33 (Original) The system of claim 19, wherein the second network device is operative to determine a length of a concatenation of an authentication protocol identifier, a user credential and the challenge, and to divide the challenge into the first part and a second part based on the determined length.

Claim 34 (Currently Amended) The system of claim 19, wherein the authentication device is integrated into the first network device ~~is operative to authenticate the user based on the final hash value~~.

Claim 35 (Currently Amended) The system of claim 19, wherein the first network device is operative to transmit a third communication including the final hash value to ~~a third network~~ the authentication device ~~configured to authenticate the user~~.

Claim 36 (Currently Amended) The system of claim 19, ~~wherein the first network device is operative to transmit the first communication within a tunnel between the first network device and the second network device~~ wherein the second network device generates a complete hash value by performing all of the hash function on the complete challenge when the second network device receives the complete challenge external to the secure network tunnel.

Claim 37 (Original) The system of claim 19, ~~wherein the second communication device is operative to transmit the second communication with a tunnel between the first device and the second device~~ wherein the second device is configured to generate a complete hash value by applying all of the hash function on the challenge when the second network device received the challenge external to the secure network tunnel.

Claim 38 (Currently Amended) A system for at least partially authenticating a user on a communications network, the system comprising:

a first communication device operative to transmit a first communication ~~from a first network device~~ to a second network device, wherein the first communication includes a challenge; and

a second network device operative to receive the challenge and to transmit a second communication from the second network device to the first network device via secure network tunnel between the first network device and the second network device, the second communication including a preliminary hash value,

wherein the second network device includes means for generating a preliminary hash value by performing only a first part of a hash function on a first part of the challenge when the second network device received the challenge via the secure network tunnel, wherein the first part of the challenge is less than the complete challenge, and

wherein the first network device includes means for ~~completing performance of the hash function~~ applying a remaining part of the hash function to the preliminary hash value, thereby producing ~~to produce~~ a final hash value; and

an authentication device that comprises means for authenticating the user based on the final hash value.

Claim 39 (Currently Amended) A computer-readable medium having computer-readable signals stored thereon that define instructions that, as a result of being executed by ~~a computer~~ one or more processors of a second network device, ~~control the computer to perform a method of at least partially authenticating a user on a communications network, the method comprising:~~ cause the one or more processors to:

(A) ~~transmitting~~ receive a first communication from a first network device that is configured to authenticate a user of the second network device based on a final hash value generated by applying a remaining part of a hash function to a preliminary hash value ~~to a second network device~~, wherein the first communication includes a challenge;

(B) generate, in response to receiving the challenge, ~~generating a~~ the preliminary hash value by performing only a first part of [[a]] the hash function on a first part of the challenge when the second network device received the challenge via a secure network tunnel between the first network device and the second network device, wherein the first part of the challenge is less than the complete challenge; and

(C) transmit ~~transmitting~~ a second communication ~~from the second network device~~ to the first network device via the secure network tunnel, the second communication including the preliminary hash value~~; and~~

~~(D) completing performance of the hash function on the first network device to produce a final hash value.~~

Claim 40 (Currently Amended) A method of at least partially authenticating a user on a communications network, the method comprising acts of:

(A) transmitting a first communication from a first network device to a second network device, wherein the first communication includes a challenge;

(B) receiving a second communication from the second network device via a secure network tunnel between the first network device and the second network device ~~to the first network device~~, the second communication including a preliminary hash value resulting from performance of only a first part of a hash function on a first part of the challenge when the second network device received the challenge via the secure network tunnel, wherein the first part of the challenge is less than the complete challenge; ~~and~~

(C) ~~completing performance~~ applying, with the first network device, a remaining part of the hash function to the preliminary hash value, thereby generating ~~on the first network device to produce~~ a final hash value; and

(D) authenticating the user based on the final hash value.

Claim 41 (Original) The method of claim 40, wherein the preliminary hash value is a result of partial performance of an Message Digest 5-based encryption function on the first part of the challenge, and wherein act (C) comprises:

completing the Message Digest 5-based encryption function.

Claim 42 (Currently Amended) The method of claim 40, wherein [[the]] complete performance of the hash function involves performing a first number of iterations, and wherein the preliminary hash value resulted from performance of a second number of iterations that is less than the first number of iterations, and

wherein act (C) includes performing a third number of iterations equal to the first number minus the second number, resulting in a complete performance of the hash function

Claim 43 (Currently Amended) The method of claim 40, wherein act (C) includes ~~completing~~ applying the remaining part of the hash function using a second part of the challenge, wherein the first part of the challenge and the second part of the challenge form the complete challenge.

Claim 44 (Currently Amended) The method of claim 40, wherein the challenge includes two parts: the first part and a second part, and the preliminary hash value is based, at least in part, on the first part of the challenge and a user credential, and the second communication includes an indication of a length in bits of the user credential, and

wherein act (C) includes ~~completing~~ applying the remaining part of the hash function based, at least in part, on the second part of the challenge and the length of the user credential.

Claim 45 (Currently Amended) The method of claim 44, wherein act (C) includes:

(1) determining a state of the hash function based, at least in part, on the length of the user credential; and

(2) ~~completing~~ applying the remaining part of the hash function based, at least in part, on the determined state.

Claim 46 (Currently Amended) The method of claim 44, wherein act (C) further comprises:

(1) determining a length of the second part of the challenge based, at least in part, on a length of the challenge and the length of the user credential; and

(2) ~~completing~~ applying the remaining part of the hash function based, at least in part, on the determined length of the second part.

Claim 47 (Currently Amended) The method of claim 40, further comprising an act of:

[[(D)]] generating the challenge on the first network device, wherein generating the challenge comprises: ~~including~~

generating a portion of the challenge having a length equal to a desired amount of entropy for the challenge, and

appending bits to the portion of the challenge to produce the challenge.

Claim 48 (Currently Amended) The method of claim 43, wherein ~~act (D) includes~~ appending bits comprises appending sixty-three bits to the challenge.

Claim 49 (Currently Amended) The method of claim 40, ~~wherein the challenge includes a plurality of sequences of bits,~~ the method further comprising an act of:

[[(D)]] generating the challenge on the first network device[[,]] such that the challenge ~~including configuring one or more of the~~ includes a plurality of sequences of bits, wherein each sequence of bits in the plurality of sequences of bits ~~to~~ includes at least one non-zero bit.

Claim 50 (Currently Amended) The method of claim 49, wherein each sequence of bits in the plurality of sequences of bits is an octet of bits.

Claim 51 (Currently Amended) The method of claim 40, further comprising an act of:

[[(D)]] generating the challenge on the first network device, wherein generating the challenge comprises ~~including~~ configuring the challenge to include at least a minimum length of bits.

Claim 52 (Canceled).

Claim 53 (Currently Amended) The method of claim 40, ~~wherein the method further comprises an act of:~~

~~(D) transmitting a third communication including the final hash value to a third network device configured to authenticate the user.~~

wherein the second network device is configured to generate a complete hash value by performing all of the hash function on the complete challenge when the second network device receives the complete challenge external to the secure network tunnel.

Claim 54 (Currently Amended) A tunnel server residing on a first network device of a communications network for at least partially authenticating a user on the communications network, the tunnel server comprising:

a challenge generator to generate a challenge that is transmitted from the first network device to a second network device;

a final hash value generator to receive via a secure network tunnel between the first network device and the second network device a preliminary hash value from the second network device, the preliminary hash value resulting from performance of only a first part of a hash function on a first part of the challenge when the second device received the challenge via the secure network tunnel, wherein the first part of the challenge is less than the complete challenge,

wherein the final hash value generator is operative to ~~complete performance~~ apply a remaining part of the hash function ~~on the first network device~~ to the preliminary hash value, thereby generating ~~to produce~~ a final hash value; and

an authenticator that authenticates the user based on the final hash value.

Claim 55 (Currently Amended) The tunnel server of claim 54, wherein the complete performance of the hash function involves performing a first number of iterations, and the preliminary hash value is the result of performance of a second number of iterations that is less than the first number of iterations, and wherein the final hash value generator is operative to perform a third number of iterations equal to the first number minus the second number, resulting in a complete performance of the hash function.

Claim 56 (Currently Amended) The tunnel server of claim 54, wherein the final hash value generator is operative to apply the remaining part of ~~complete~~ the hash function using a second part of the challenge, wherein the first part of the challenge and the second part of the challenge form the complete challenge.

Claim 57 (Currently Amended) The tunnel server of claim 54, wherein the challenge includes the first part and a second part, and the second communication includes an indication of a length in bits of a user credential, and

wherein the final hash value generator is operative to apply the remaining part of ~~complete~~ the hash function based, at least in part, on the second part of the challenge and the length of the user credential.

Claim 58 (Currently Amended) The tunnel server of claim 57, wherein the final hash value generator is operative to determine a state of the hash function based, at least in part, on the length of the user credential, and to ~~for complete~~ apply the remaining part of the hash function based, at least in part, on the determined length.

Claim 59 (Currently Amended) The tunnel server of claim 57, wherein the final hash value generator is operative to determine a length of the second part of the challenge based, at least in part, on a length of the challenge and the length of the user credential, and to ~~complete~~ apply the remaining part of the hash function based, at least in part, on the determined length of the second part of the challenge.

Claim 60 (Original) The tunnel server of claim 54, wherein the challenge generator is operative to generate the challenge, to generate a portion of the challenge having a length equal to a desired amount of entropy for the challenge, and to append bits to the portion of the challenge to produce the challenge.

Claim 61 (Original) The tunnel server of claim 60, wherein the challenge generator is operative to append sixty-three bits to the portion.

Claim 62 (Currently Amended) The tunnel server of claim 54, wherein ~~the challenge includes a plurality of sequences of bits, and~~ the challenge generator is operative to generate the challenge[[,]] ~~and to configure one or more of~~ such that the challenge includes a ~~the~~ plurality of sequences of bits, wherein each sequence of bits in the plurality of sequences of bits ~~to~~ includes at least one non-zero bit.

Claim 63 (Currently Amended) The tunnel server of claim 62, wherein each sequence of bits in the plurality of sequences of bits is an octet of bits.

Claim 64 (Currently Amended) The tunnel server of claim 54, wherein the challenge generator is operative to generate the challenge~~, including configuring~~ such that the challenge [[to]] includes at least a minimum length of bits.

Claim 65 (Canceled).

Claim 66 (Original) The tunnel server of claim 54, wherein the tunnel server is operative to control transmission of a third communication including the final hash value to a third network device configured to authenticate the user.

Claim 67 (Currently Amended) The tunnel server of claim 54, ~~wherein the tunnel server is operative to control transmission of the first communication within a tunnel between the first network device and the second network device.~~ wherein the second network device is configured to generate a complete hash value by performing all of the hash function on the complete challenge when the second network device receives the complete challenge external to the secure network tunnel.

Claim 68 (Currently Amended) A tunnel server residing on a first network device of a communications network for at least partially authenticating a user on the communications network, the tunnel server comprising:

a challenge generator to generate a challenge that is transmitted from the first network device to a second network device, wherein the tunnel server is operative to receive a preliminary hash value from the second network device via a secure network tunnel between the first network device and the second network device, the preliminary hash value resulting from performance of only a first part of a hash function on a first part of the challenge when the second network device received the challenge via the secure network tunnel, wherein the first part is less than the complete challenge; ~~and~~

means for applying a remaining part ~~completing performance~~ of the hash function to the preliminary hash value, thereby generating ~~on the first network device to produce~~ a final hash value; and

means for authenticating the user based on the final hash value.

Claim 69 (Currently Amended) A computer-readable medium having computer-readable signals stored thereon that define instructions that, as a result of being executed by a first network device ~~computer~~, control the first network device ~~computer~~ to perform a method of at least partially authenticating a user on a communications network, the method comprising acts of:

(A) transmitting a first communication from [[a]] the first network device to a second network device, wherein the first communication includes a challenge;

(B) receiving a second communication from the second network device to the first network device via a secure network tunnel between the first network device and the second network device, the second communication including a preliminary hash value generated by performing only a first part of a hash function on a first part of the challenge when the second network device received the challenge via the secure network tunnel, wherein the first part of the challenge is less than the complete challenge; and

(C) ~~completing performance~~ applying a remaining part of the hash function to the preliminary hash value on the first network device, thereby generating ~~to produce~~ a final hash value.

Claim 70 (Currently Amended) A method of at least partially authenticating a user on a communications network in response to a challenge received at a second network device from a first network device, the method comprising acts of:

receiving a challenge from a first network device that is configured to authenticate a user of the second network device based on a final hash value generated by applying a remaining part of a hash function to a preliminary hash value;

[[(A)]] generating [[a]] the preliminary hash value by performing only a first part of a hash function on a first part of the challenge when the second network device received the challenge via a secure network tunnel between the first network device and the second network device, wherein the first part of the challenge is less than the complete challenge; and

[[(B)]] transmitting a communication from the second network device to the first network device via the secure network tunnel, the communication including the preliminary hash value.

Claim 71 (Currently Amended) The method of claim 70, wherein ~~act (A)~~ generating the preliminary hash value comprises:

performing only part of a Message Digest 5-based encryption function.

Claim 72 (Currently Amended) The method of claim 71, ~~wherein a standard Message Digest 5 algorithm includes adding an appendage of information to information to be communicated to produce padded information that has a length that is a multiple of sixty-four octets, and includes inputting the padded information to a standard Message Digest 5 function, and~~ wherein ~~act (A)~~ generating the preliminary hash value comprises:

(1) generating an input sequence to the Message Digest 5-based encryption function by concatenating information to be communicated from the second network device to the first network device; and

(2) inputting the input sequence into the Message Digest 5-based encryption function without previously adding an appendage of information to the input sequence.

Claim 73 (Currently Amended) The method of claim 70, wherein the complete performance of the hash function involves performing a first number of iterations, and wherein generating the preliminary hash value comprises ~~act (A) includes~~ performing a second number of iterations that is less than the first number of iterations.

Claim 74 (Currently Amended) The method of claim 70, wherein ~~act (A) includes~~ generating the preliminary hash value comprises generating the preliminary hash value based, at least in part, on the first part of the challenge and a user credential.

Claim 75 (Currently Amended) The method of claim 74, wherein ~~act (A) includes~~ generating the preliminary hash value comprises dividing the challenge into the first part and a second part, and the method further comprises:

[[(E)]] configuring the communication to include an indication of a length in bits of the user credential.

Claim 76 (Currently Amended) The method of claim 70, wherein ~~act (A)~~ generating the preliminary hash value comprises:

(1) determining a length of a concatenation of an authentication protocol identifier, a user credential and the challenge; and

(2) dividing the challenge into the first part of the challenge and a second part of the challenge based on the determined length.

Claim 77 (Currently Amended) The method of claim 70, ~~wherein act (A) includes transmitting the first communication within a tunnel between the first network device and the second network device.~~ further comprising generating, with the second network device, a complete hash value by performing all of the hash function on the complete challenge when the second network device receives the complete challenge external to the secure network tunnel.

Claim 78 (Currently Amended) A client residing on a second network device of a communications network, ~~for at least partially authenticating a user in response to a challenge received on the second network device from a first network device,~~ the client comprising:

an interface that receives a challenge from a first network device that is configured to authenticate a user of the second network device based on a final hash value generated by applying a remaining part of a hash function to a preliminary hash value;

a preliminary hash generator to generate [[a]] the preliminary hash value by performing only a first part of [[a]] the hash function on a first part of the challenge when the client received the challenge via a secure network tunnel between the first network device and the second network device, wherein the first part of the challenge is less than the complete challenge,

wherein the second network device is operative to transmit a communication from the second network device to the first network device via the secure network tunnel, the communication including the preliminary hash value.

Claim 79 (Original) The client of claim 78, wherein the preliminary hash generator is operative to perform only part of a Message Digest 5-based encryption function.

Claim 80 (Currently Amended) The client of claim 79, ~~wherein a standard Message Digest 5 algorithm includes adding an appendage of information to information to be communicated to produce padded information that has a length that is a multiple of sixty-four octets, and includes inputting the padded information to a standard Message Digest 5 function, and~~

wherein the preliminary hash generator is operative to generate an input sequence to the Message Digest 5-based encryption function by concatenating information to be communicated from the second network device to the first network device, and to input the input sequence into the Message Digest 5-based encryption function without previously adding an appendage of information to the input sequence.

Claim 81 (Original) The client of claim 78, wherein the complete performance of the hash function involves performing a first number of iterations, and

wherein the preliminary hash generator is operative to perform a second number of iterations less than the first number of iterations.

Claim 82 (Original) The client of claim 78, wherein the preliminary hash generator is operative to generate the preliminary hash value based, at least in part, on the first part of the challenge and a user credential.

Claim 83 (Original) The client of claim 82, wherein the preliminary hash generator is operative to divide the challenge into the first part and a second part, and to configure the communication to include an indication of a length in bits of the user credential.

Claim 84 (Original) The client of claim 78, wherein the preliminary hash generator is operative to determine a length of a concatenation of an authentication protocol identifier, a user credential and the challenge, and to divide the challenge into the first part and a second part based on the determined length.

Claim 85 (Currently Amended) The client of claim 78, wherein the client is operative to ~~control transmission of the first communication within a tunnel between the first network device and the second network device.~~ generate a complete hash value by performing all of the hash function on the complete challenge when the second network device receives the complete challenge external to the secure network tunnel.

Claim 86 (Currently Amended) A client residing on a second network device of a communications network, ~~for at least partially authenticating a user in response to a challenge received on the second network device from a first network device,~~ the client comprising:

means for receiving a challenge from a first network device that is configured to authenticate a user of the second network device based on a final hash value generated by applying a remaining part of a hash function to a preliminary hash value;

means for generating [[a]] the preliminary hash value by performing only a first part of [[a]] the hash function on a first part of the challenge when the client received the challenge via a secure network tunnel between the first network device and the second network device, wherein the first part is less than the complete challenge,

wherein the second network device is operative to transmit a communication from the second network device to the first network device via the secure network tunnel, the communication including the preliminary hash value.

Claim 87 (Currently Amended) A computer-readable medium having computer-readable signals stored thereon that define instructions that, as a result of being executed by a second network device ~~computer~~, control the second network device ~~computer~~ to: ~~perform a method of at least partially authenticating a user on a communications network in response to a challenge received at a second network device from a first network device, the method comprising acts of~~:

receive a challenge from a first network device that is configured to authenticate a user of the second network device based on a final hash value generated by applying a remaining part of a hash function to a preliminary hash value;

~~(A) generating a~~ generate the preliminary hash value by performing only a first part of [[a]] the hash function on a first part of the challenge when the second network device received the challenge via a secure network tunnel between the first network device and the second network device, wherein the first part of the challenge is less than the complete challenge; and

~~(B) transmitting~~ transmit a communication from the second network device to the first network device via the secure network tunnel, the second communication including the preliminary hash value.